IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re:	U.S. Patent Application of Tet Hin YEAP *et al.*		
App. No.:	10/673,509	Group Art Unit:	2155
Filed:	September 30, 2003	Examiner:	Shawki Saif ISMAIL
For:	SYSTEM AND METHOD FOR SECURE ACCESS		

APPEAL BRIEF UNDER 37 CFR §41.37

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Further to the Notice of Appeal filed April 10, 2008, submitted herewith is an Appeal Brief in accordance with 37 CFR §41.37. The fee for filing a brief in support of an appeal as set forth in 37 CFR §41.20(b)(2) is also being filed herewith.

A petition for extension of time is being filed concurrently herewith.

If any further fees are due, the Director is hereby authorized to debit the required amount from deposit account no. 19-2550 and to advise the Applicant accordingly.

07/11/2008 HMARZI1 00000015 192550 10673509
01 FC:1402 510.00 DA

I. 37 CFR §41.37 (c)(1)(i) - Real Party in interest

The real party in interest is the assignee of the entire interest in the U.S. patent application, namely BCE, Inc.

II. 37 CFR §41.37 (c)(1)(ii) - Related Appeals and Interferences

The Applicant believes that there are no appeals or interferences that are related to, or may directly affect, or be affected by, or have a bearing on the Board's decision in the pending appeal.

III. 37 CFR §41.37 (c)(1)(iii) - Status of the Claims

The following is a statement of the current status of the claims that have been filed in the present application:

Claims 35-42, 44-50 and 52-82 are currently rejected.

No claims are considered allowable by the Examiner.

Claims 1-34, 43 and 51 are cancelled.

The text of claims 35-42, 44-50, 52-82 can be seen in Section VIII entitled "Claims Appendix", included below.

The rejection of claims 35-42, 44-50, 52-82 is being appealed.

IV. 37 CFR §41.37 (c)(1)(iv) - Status of Amendments

No amendments were filed in response to the final Office Action of January 10, 2008. In addition, no amendments were filed subsequent to the filing of the response to the final Office Action.

The last amendments to the claims were made in the Applicant's communication to the Patent Office dated October 1, 2007, which was made in response to the non-final Office Action of July 2, 2007.

V. 37 CFR §41.37 (c)(1)(v) - Summary of Claimed Subject Matter

The present application includes 46 claims, of which independent claims 35, 45, 56, 67, 68, 70, 72, 74 are being appealed. A summary of independent claims 35, 45, 56, 67, 68, 70, 72, 74 is provided below. References in brackets refer to the specification and drawings as originally filed.

Claim 35

Claim 35 is directed to an authentication system (Fig 1, 30). The authentication system comprises an access controller (Fig 1, 54; ¶0014) that is operable to communicate with a client (Fig 1, 42; ¶0016) via a first communication medium (¶0014; ¶0063-0065). The authentication system further comprises an authentication server (Fig 1, 38; ¶0015) that is operable to communicate with the client and the access controller via a second communication medium (¶0015; ¶0063-0065). The authentication server is further operable to deliver a first key to the client (Fig. 3, 355; ¶0048) and a second key to the access controller (Fig 2, 240; ¶0027). The second key is complementary to the first key (¶0015) such that when the client and the access controller are connected, communications therebetween can be encrypted using the keys (¶0015, ¶0016; Fig 4, 420-430; ¶0052-0053; ¶0060). The access controller is further operable to selectively pass instructions received from the client to a computer attached to the access controller if a verification protocol utilizing the keys is met (Fig 4, 435-440; ¶0054-0055). The first key is delivered to the client only if a user operating the client authenticates the user's identity with the server (Fig 3, 310-355; ¶0043-0048).

Claim 45

Claim 45 is directed to an access controller (Fig 1, 54) for intermediating communications between an interface and a computer (¶0017) and operable to store a second key complementary to a first key (Table 1; Fig 1, 62; ¶0018-0019; Table III; ¶0032). The access controller is further operable to communicate with a client via the interface (Fig 1, 58; ¶0014). The client is operable to store the first key (Table V; Fig 1, 70; ¶0016; ¶0039; Table VII) and to receive instructions from a user (¶0051). The access controller is still further operable to selectively pass the instructions to the computer if a verification protocol utilizing the keys is met (Fig 4, 435-440; ¶0054-0055). The verification protocol includes the generation of a random number by the client and an encryption of the random number by the client using the first key (Fig. 4, 415-420; ¶0052). The random number and the encrypted random number are delivered from the client to the access controller (Fig. 4, 425; ¶0052). The encrypted random number is decrypted using the second key by the access controller (Fig. 4, 430; ¶0053) and a comparison of the random number and the decrypted number is made (Fig. 4, 435; ¶0054). If the comparison finds a match of the random number with the decrypted random number, the decision is made to pass at least a portion of the instructions (Fig. 4, 435-440; ¶0054-0055). If no match is found, a decision is made not to pass the at least a portion of the instructions (Fig. 4, 435; ¶0054).

Claim 56

Claim 56 is directed to a method (Fig. 2, 200; ¶0023-0035), in an authentication server (Fig 1, 28; ¶0015), of securing access between a client (Fig 1, 42; ¶0016) having temporary connection to a computer (Fig 1, 50; ¶0014; ¶0066) via an access controller (Fig 1, 54; ¶0014). The access controller is for selectively passing instructions received from the client to the computer if a verification protocol utilizing a set of keys is met (¶0017; Fig. 4, 435-440; ¶0054-0055). The method comprises receiving a request from the access controller for an updated first key (Fig. 2, 220; ¶0025-0025). The request is authenticated (Fig. 2, 220; ¶0025). The updated first key and a second key corresponding to the updated

first key are determined (Fig. 2, 230; ¶0026). The updated first key is delivered to the access controller (Fig. 2, 240; ¶0027).

Claim 67

Claim 67 is directed to a method (Fig. 4, 400; ¶0050-0056) of securing access between a client (Fig. 1, 42; ¶0016) and a computer (Fig. 1, 34, 50; ¶0014; ¶0066) having an access controller (Fig 1, 54; ¶0014) intermediate the client and the computer. The client receives an instruction destined for the computer (Fig. 4, 410; ¶0051) and generates a random number (Fig. 4, 415, ¶0052). The client encrypts the random number using a first key (Fig.4, 420; ¶0052). The random number, the encrypted random number and the instruction are delivered to the access controller (Fig. 4, 425; ¶0052). The access controller decrypts the encrypted random number using a second key, the second key being complementary to the first key (Fig. 4, 430; ¶0053). The random number and the decrypted number are compared (Fig. 4, 435; ¶0054). If the comparison finds a match of the random number with the decrypted number, at least a portion of the instruction is passed to the computer (Fig. 4, 440; ¶0054-0055). If no match is found, the at least a portion is discarded (Fig. 4, path "Discard Instruction"; ¶0054).

Claim 68

Claim 68 is directed to an authentication server (Fig 1, 38; ¶0015) comprising an interface (¶0015) for communicating with a client and an access controller via a communication medium (Fig. 1, 46) and a processing unit (¶0015). The processing unit is operable to determine a first key for delivery to the client and a second key for delivery to the access controller (¶0015; ¶0026). The first key is delivered to the client only if a user operating the client authenticates the user's identity with the server (Fig 3, 310-355; ¶0043-0048). When the access controller and the client are connected, the access controller selectively passes instructions from the access controller if a verification protocol utilizing the keys is met (¶0017; Fig. 4, 435-440; ¶0054-0055).

Claim 70

Claim 70 is directed to an authentication server (Fig 1, 38; ¶0015) for securing access between a client (Fig. 1, 42; ¶0016) having temporary connection and a computer (Fig 1, 50; ¶0014; ¶0066) via an access controller (Fig 1, 54; ¶0014). The access controller is for selectively passing instructions received from the client to the computer if a verification protocol utilizing a set of keys is met (¶0017; Fig. 4, 435-440; ¶0054-0055). The authentication server comprises means for receiving a request from the access controller for an updated first key (¶0014-0015 Fig. 2, 220; ¶0025-0025), means for authenticating the request (¶0015; Fig. 2, 220; ¶0025), means for determining the updated first key and a second key corresponding to the updated first key (¶0015; Fig. 2, 230; ¶0026), and means for delivering the updated first key to the access controller (¶0014-15; Fig. 2, 240; ¶0027).

Claim 72

Claim 72 is directed to a method (Fig. 5, 500; ¶0057-0059), in an access controller (Fig 1, 54; ¶0014) for selectively passing instructions between a client (Fig. 1, 42; ¶0016) and a computer (Fig 1, 50; ¶0014; ¶0066) if a verification protocol is met (¶0017; Fig. 4, 435-440; ¶0054-0055), of expiring the verification protocol. The method comprises determining if a first preset period of time since the client disconnected from the access controller has elapsed (Fig. 5, 510; ¶0057). The method also comprises determining if a second preset period of time since the verification protocol was updated has elapsed (Fig. 5, 520; 0058). The verification protocol is expired by refusing to pass the instructions if either of the preset periods of time have elapsed (Fig. 5, 515; ¶0057-0058).

Claim 74

Claim 74 is directed to an authentication system (Fig 1, 30). The authentication system comprises an access controller (Fig 1, 54; ¶0014) that is operable to communicate with a client (Fig 1, 42; ¶0016) via a first communication medium

(¶0014; ¶0063-0065). The authentication system further comprises an authentication server (Fig 1, 38; ¶0015) that is operable to communicate with the client and the access controller via a second communication medium (¶0015; ¶0063-0065). The authentication server is further operable to deliver a first key to the client (Fig. 3, 355; ¶0048) and a second key to the access controller (Fig 2, 240; ¶0027). The second key is complementary to the first key (¶0015) such that when the client and the access controller are connected, communications therebetween can be encrypted using the keys (¶0015, ¶0016; Fig 4, 420-430; ¶0052-0053; ¶0060). The access controller is further operable to selectively pass instructions received from the client to a computer attached to the access controller if a verification protocol utilizing the keys is met (Fig 4, 435-440; ¶0054-0055). The access controller contains a preset second key (Table I; Fig 1, 62; ¶0017-0019) and the authentication server maintains a record of the preset second key (Table II; Fig. 1, 66; ¶0021-0022). The authentication server is operable to deliver the first key and the second key only if the access controller successfully transmits the preset second key to the authentication server and the transmitted preset second key matches the authentication server's record thereof (Fig. 2, 200; ¶0023-0035).

VI. 37 CFR §41.37 (c)(1)(vi) - Grounds of rejection to be reviewed on Appeal

In the final Office Action dated January 10, 2008, the Examiner has rejected claims 35-42, 44-50 and 52-82 under 35 U.S.C. §102(e) as being anticipated by US Patent Application Publication no. 2003/0056096A1 (hereafter to be referred to as Albert).

VII. 37 CFR §41.37 (c)(1)(vii) - Arguments

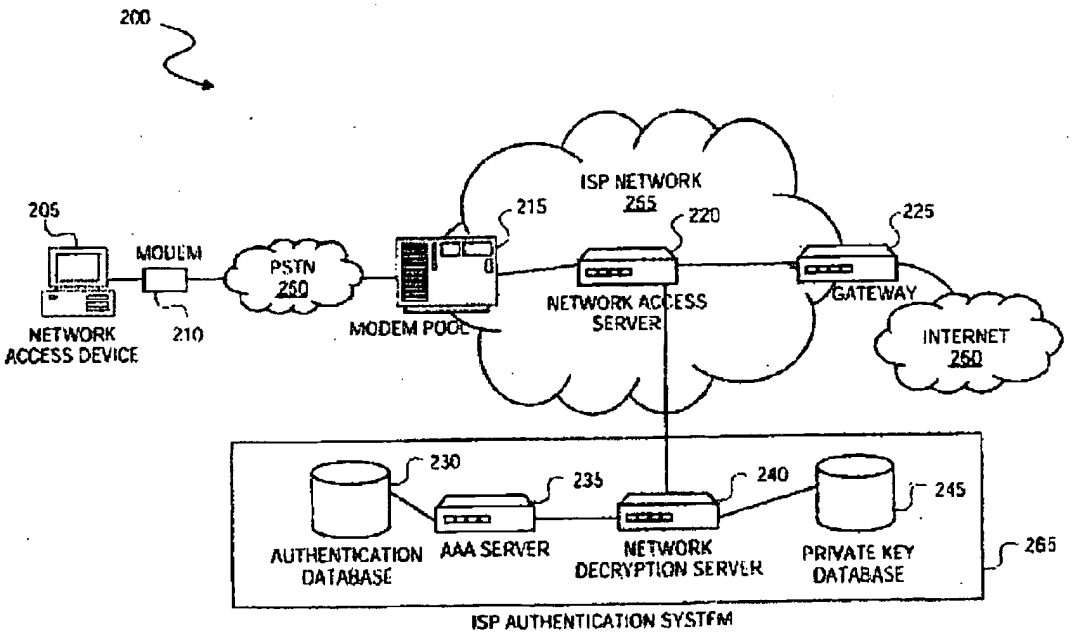
Response to Rejection of claim 35-42, 44-50 and 52-82 under 35 U.S.C. §102(e)

The Examiner has rejected claims 35-42, 44-50 and 52-82 under 35 USC §102(e) as being anticipated by Albert.

For the reasons presented below, the Applicant respectfully disagrees with and traverses the Examiner's rejection, and submits that claims 35-42, 44-50 and 52-82, as they currently stand, are in allowable form.

Brief synopsis of Albert

Albert discloses a system for authenticating network user credentials. The system in Albert is to be used, for example, by an Internet Service Provider (ISP) to verify the identity of dial-up internet customers prior to providing them access to the internet using the ISP's equipment.



The Albert System

The above figure, corresponding to Figure 2 of Albert, shows the system of Albert. As shown, the Albert system comprises an ISP authentication system 265 consisting of an authentication server (AAA server) 235 and a network decryption server 240, each having a respective database. The ISP authentication system 265 is connected to a network access server (NAS) 220 that is in turn connected any number of network access devices 205 (only one shown/discussed, for simplicity). The network access device 205 may be, for example, a computer that is used by a user to access dial-up internet services. These services are provided by the NAS 220 if the user's credentials can first be successfully authenticated by the ISP authentication system 265. [Albert ¶ 0055]

The Basic System:
In order to gain access to the internet, a network access device 205 first encrypts a password, entered by the user, using a public key from a public/private key pair. The network decryption server 240's database indexes private keys by user names so there may be up to one public/private key pair per user. In practice, there may be one public/private key pair per ISP. In either case, the public/private key pair used to encrypt the user's password is referred to herein as the ISP authentication system 265's public/private keys since that is where the pair is generated. [Albert ¶ 0101]

The network access device 205 sends the encrypted password along with a user ID, also entered by the user, to the NAS 220. As shown in the above figure, the NAS 220 forms a link between the network access device 205 and the internet, but it relies on the ISP authentication system 265 to determine whether a particular user is permitted access. Specifically, upon receiving the user's ID and encrypted password, the NAS 220 forwards this data to the ISP authentication system 265 where it is received by the network decryption server 240. The network decryption server 240 has a database of private keys 245, each private key therein corresponding to a different public key and being indexed by at least one user name. The network decryption server 240 locates the right private key

in the database (using the received user ID as an index) and uses it to decrypt the password received. [Albert ¶ 0062] The network decryption server 240 then forwards the user ID and decrypted password to an authentication server (AAA server) 235 (still within the ISP authentication system 265) which has an official password for each user stored in an authentication database 230. If the AAA server 235 finds a match between the official password and the transmitted password, instructions are sent, through the network decryption server 240, to the NAS 220 to allow the network access device 205 to access the internet. [Albert ¶ 0063]

This system, Albert suggests, may be combined with existing authentication protocols such as PAP/RADIUS and CHAP/RADIUS.

PAP/RADIUS:

The system described above can be implemented to work with the PAP and RADIUS protocols. In such a case, authentication begins with the network access device 205 creating a PAP packet containing the user ID and the password, encrypted as before. This packet is sent to the NAS 220, which makes a RADIUS packet with the information and forwards this packet to the ISP authentication system 265. [Albert ¶ 0062] Symmetric encryption takes place between the NAS 220 and the ISP authentication system 265, whereby a common key is used on both ends to lock and unlock packet contents. [Albert ¶ 0008]

CHAP/RADIUS:

Alternatively, the system described above may employ the slightly more secure CHAP protocol along with RADIUS. With such an arrangement, the NAS 220 must first send the network access device 205 a number that it has randomly generated. The network access device 205 uses this random number to generate a non-reversible hash of the password it received from the user, and encrypts this hash in the same manner as the password was encrypted above. The

network access device 205 then creates a CHAP packet containing the user ID and the encrypted hashed password, and sends it to the NAS 220. The NAS 220 receives this packet and prepares a RADIUS packet containing the user ID and encrypted hashed password along with the random number generated earlier. This RADIUS packet is sent to the ISP authentication system 265 where it is received by the network decryption server 240. The network decryption server 240 decrypts the encrypted hashed password and replaces the password field of the RADIUS packet with the result. The RADIUS packet, now containing the user ID, the hashed (but decrypted) password and the random number, is then forwarded to the AAA server 235. The AAA server 235 now retrieves the user's official password from the authentication database 230 and hashes it using the random number from the RADIUS packet. The result is compared to the hashed (but decrypted) password received from the network decryption server 240 to determine whether the user has provided the correct password and may be given access to the internet. [Albert ¶ 0066]

Brief Discussion of Certification Authorities Described in Kaufman *et al.*

In addition to Albert, the Examiner also relies on an excerpt of Kaufman *et al.*'s "Network Security, Private Communication in a Public World" Second Edition, ISBN 0-13-046019-2, published by Prentice Hall PTE in 2002 (the cited excerpt hereinafter referred to as the NPL document) to support his rejection of the claims.

The NPL document presents a 1-page basic introduction of Certification Authorities (also known as Certificate Authorities or CAs). As explained in the NPL document, CAs exist to prevent intruders from impersonating an online resource (e.g. an online banking service). An intruder impersonates an online resource by emitting a fake public key (to which the intruder has the corresponding private key) and convincing a prospective user of the online resource that this fake key is the public key of the online resource. [NPL document p. 228 ¶ 1] If the scheme is successful, the prospective user of the

online resource will begin encrypting data intended for the online resource with the fake key, and sending it. The intruder then intercepts or receives this data and decrypts it using the private key corresponding to the fake key. In such a way, an intruder can gain access to the user's password or other sensitive information. The potential for this kind of fraud creates a need for a mechanism that allows prospective users of an online resource to reliably obtain online the public key of the online resource. It is this need that CAs are meant to address.

In particular, CAs act as a trusted verifier of online resources' public keys. They obtain online resources' public keys from online resources via a safe transfer medium (e.g. hand delivered and notarised for authenticity). For each online resource that is registered with a CA, the CA generates a digital certificates to be made generally available (e.g. somewhere on the internet) that contains the online resource's public key in a format unforgeably signed. To sign the digital certificate the CA uses its own private key, known to nobody else in the world. Anybody wanting to read the digital certificate must have the CA's public key, which preferably is known to everyone. (Digital signing resembles encryption but unlike in encryption, in digital signature it is the private key that encrypts the digital signature and the public key that can decrypt it.) Thus to read a digital certificate, one must have the emitting CA's public key. [NPL document p.228 ¶ 2] No particular means is provided in the NPL document to obtain the CA's public key safely, but if it can be obtained, it allows the bearer to validate all the digital certificates emitted by the CA and thus obtain the online resource's public key contained in each such digital certificate. Hence the CA's public key allows safe access to the public keys of all the resources registered with the CA.

In practice, digital certificates contain the public key that is sought, the name/location of the resource associated with the public key and the digital signature which, as explained above, is created using the CA's private key. The digital certificates may be stored anywhere, such as with the CA or with the resource they correspond to. [NPL document p.228 ¶ 2]

1) Claims 35-42 and 44

The Examiner's attention is respectfully directed towards the following features of independent claim 35:

> **Claim 35**
> An authentication system comprising:
> an access controller operable to communicate with a client via a first communication medium; and
> an authentication server operable to communicate with said client and said access controller via a second communication medium and further **operable to generate a first key for delivery to said client and a second key for delivery to said access controller, said second key being complementary to said first key** such that when said client and said controller are connected, communications therebetween can be encrypted using said keys; and wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met;
> **wherein said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server.**

As will be demonstrated in detail below, the Applicant respectfully submits that:

i. the combination of Albert and the NPL document in a rejection under 35 USC 102(e) is improper;

ii. the cited prior art does not teach or suggest the feature of *an authentication server operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key*; and

iii. the cited prior art does not teach or suggest the feature of *said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server.*

i. The combination of Albert and the NPL document in a rejection under 35 USC 102(e) is improper

In his rejection under 35 USC 102(e), the Examiner has combined Albert with the NPL document, alleging that the NPL document shows that a certain feature missing in Albert is actually inherent in Albert though not expressly disclosed. The Applicant respectfully disagrees with the Examiner's interpretation of the prior art and submits that the NPL document is concerned with different technology than Albert and thus cannot be used to show that a feature is inherent in Albert.

As mentioned above, the NPL document provides a basic introduction to Certification Authorities, which are third party systems used to counter the emission of fake public keys online [NPL document p.228 ¶ 2]. Albert, on the other hand, relates to a self-contained system for authorising access to an online resource. In particular, Albert provides a system for verifying the identity of users of dial-up internet service when they log on to the internet. Advantageously, the verification method provided can be used by the ISP without substantial recourse to external services, even when the user is logging into a foreign network. [Albert ¶ 0058, ¶ 0071] One of the objectives of Albert is to provide a system that does not require the use of external services such as Certification Authorities, the need of which is specifically pointed out as a disadvantage of the art prior to Albert. [Albert ¶ 0014]

Besides specifically teaching away from employing Certification Authorities, the Albert reference does not teach anything that resembles a CA. To begin with, Albert does not aim to protect a public key at all but rather to protect, by encryption, the password of a user logging on. [Albert ¶ 0056] Whereas CAs protect users from supposititious online resources, Albert aims to protect an online resource from unauthorized users.

Albert achieves his goal by having the password encrypted at the user end (network access device 205) before sending it to an ISP authentication system 265 that decrypts it and decides whether or not to allow access to a resource (the

internet). [Albert ¶ 0055] In contrast, a Certification Authority merely generates digital certificates comprising a public key for an online resource. The digital certificate is not used by the online resource provider to determine if a user is entitled to access the online resource, rather it is used by a user to find out the online resource's public key. [NPL document p.228 ¶ 2] The online resource's public key allows the user to communicate safely with the online resource but is generally available to everyone (who has the CA's public key). However, having the online resource's public key does not mean that the user will be allowed access to the corresponding online resource.

The NPL document also describes, on page 227, Key Distribution Centers (KDCs), which are more primitive alternatives to CAs. But the section on KDCs is not relied upon by the Examiner and is only used within the NPL document to provide context for the discussion on CAs. Furthermore, KDCs are even more conceptually distant from the Albert system than CAs and thus there is no need to discuss KDCs in further detail here.

In the Advisory Action mailed March 28, 2008, the Examiner states that he employs the NPL reference in accordance with MPEP 2131.01 in order to show that a characteristic not disclosed in Albert is actually inherent in the Albert system. Yet Albert discloses a system that is significantly different than a CA and that does not use CAs. The Applicant respectfully submits that since Albert does not teach or employ Certification Authorities or like structures (or KDCs), a document describing only such Certification Authorities (and KDCs) cannot possibly show that any particular feature is inherent in the Albert system.

In light of the foregoing, the Applicant respectfully submits that the Examiner improperly combined documents for his rejection under 35 USC 102(e) and that accordingly, the rejection of claim 35 cannot stand.

ii. The cited prior art does not teach or suggest the feature of an authentication server operable to deliver a first key to a client and a second key to an access controller, said second key being complementary to said first key

On page 3 of the Office Action dated January 10, 2008, the Examiner alleges that the above-noted feature is disclosed in Albert. As explanation for this allegation, he merely refers to paragraphs 0060 and 0061 of Albert. In these paragraphs, it is explained that the network access device 205 sends the user's password in encrypted form using a specific prior-art encryption technique, and the specific encryption technique is then described. However, the presence of encryption in Albert alone is not sufficient to anticipate the claimed invention and the Applicant respectfully submits that Albert fails to teach or suggest an authentication server operable to deliver a first key to a client and a second key to an access controller, with the second key being complementary to the first key.

Indeed, a person of ordinary skill in the art searching for similarities between Albert and the present invention, employing any interpretation of the prior art and considering Albert in every form (including in combination with each prior-art protocol suggested in Albert), would find that none of the elements in the system of Albert are operable to deliver a first key to a client and a second key to an access controller, said second key being complementary to said first key. This feature is completely absent from Albert.

In the Basic System:
For the aforesaid feature to be present in Albert, the ISP authentication system 265, a component thereof, or another element would need to "deliver a first key to a client and a second key to an access controller." Yet in the basic system, Albert does not suggest that the ISP authentication system 265 (or any other element) deliver any encryption key to any recipient. Rather, Albert merely discloses that the network access device 205 knows the ISP authentication

system 265's public key, which is complementary to the ISP authentication system 265's private key, held in the ISP authentication system 265 (see the first three lines of ¶ 0062 in Albert). There is no indication, however of where the private/public keys are generated and there is no indication that a key is sent to the network access device 205 from the ISP authentication system 265 (or vice versa). Yet even if Albert did teach the ISP authentication system 265 sending the public key to the network access device 205, a skilled reader would still not be brought closer to the claimed invention since neither ISP authentication system 265 nor any constituent part thereof delivers a second key to any recipient whatsoever. There is therefore no "[delivery of] a second key to an access controller". Thus, it is respectfully submitted that the above-noted feature is completely absent from Albert.

Using PAP/RADIUS:

If the PAP and RADIUS protocols are used with the Albert system, communications between the ISP authentication system 265 and the NAS 220 are done using the RADIUS protocol which, according to Albert, calls for symmetric encryption. Albert explains that here, encryption/decryption is done at both ends using the same key, which shall be referred to herein as the RADIUS key. [Albert ¶ 008, ¶ 0065] Albert does not provide any indication as to how the NAS 220 and the ISP authentication system 265 come to agree on the common RADIUS key to be used and Albert does not suggest that the ISP authentication system 265, or any constituent thereof, delivers the RADIUS key to the NAS 220 (or vice versa). Thus where Albert describes using the RADIUS protocol, it does not provide any teachings that would bring a skilled reader closer to the claimed invention.

Furthermore, even if Albert did suggest delivery of the RADIUS key from the ISP authentication system 265 to the NAS 220 (or vice versa), Albert would still not harm the present claim since the RADIUS key thus sent would be in no way complementary, or even related, to any other key that could potentially be seen

as sent by the ISP authentication system 265 (or the NAS 220). Specifically, there would still be absolutely no relationship between the RADIUS key and the ISP authentication system 265's public key (which, in any case, is not shown to be delivered out by the ISP authentication system 265). Thus, in addition to lacking the delivery by one element of two different keys to two respective destinations (fails to teach "an authentication server operable to deliver a first key to a client and a second key to an access controller"), the Albert system using the PAP and RADIUS protocols is also devoid of two delivered keys having a complementary relationship (fails to teach "said second key being complementary to said first key").

Using CHAP/RADIUS

If the CHAP and RADIUS protocols are used with the Albert system, communication between the NAS 220 and ISP authentication system 265 still employs the RADIUS protocol, but the system security is augmented by the use of CHAP. As described in the brief synopsis of Albert, above, in this scheme the NAS 220 generates a random number and sends it to the network access device 205. The NAS 220 later receives user credentials (including the user password hashed using the random number) from the network access device 205 and forwards these along with the previously-generated random number to the ISP authentication system 265 (specifically, to the network decryption server 240 therein). [Albert ¶ 0066] Thus it is the NAS 220 that sends the random number to both the network access device 205 and the ISP authentication system 265. [Albert ¶ 0067] But the NAS 220 does not perform any authentication function; the random number is never delivered by an "authentication server" as claimed.

Inside the ISP authentication system 265, when the ISP authentication system 265 receives the random number (and protected user credentials) from the NAS 220, it is received by the network decryption server 240. This server merely performs decrypting function and is not responsible for authentication. [Albert ¶ 0067] Rather, the network decryption server 240 forwards the credentials, once

decrypted, along with the random number to the AAA server that itself determines whether the password entered by the user was correct. [Albert ¶ 0068]

The random number used in CHAP is delivered by the NAS 220, which (like all other elements of the Albert system) does not deliver out any of the other keys (the RADIUS key and the ISP authentication system 265's public/private key). However, even if Albert did teach the NAS 220 delivering one or both of these keys, the addition of the CHAP protocol would still fail to bring a reader closer to the claimed invention since the random number delivered by the NAS 220 for the CHAP protocol is, by definition, random and therefore not complementary but completely unrelated to the RADIUS key and the ISP authentication system 265's public/private key. Thus the use of the CHAP and RADIUS protocols with the system of Albert brings a reader no closer to a system involving the delivery of a first key and the delivery of a second key, complementary to the first.

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest an authentication server operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key. Therefore, it is respectfully submitted that the rejection of claim 35 under 35 USC 102(e) cannot stand.

iii. The cited prior art does not teach or suggest the feature of said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server

On page 3 of the Office Action, the Examiner appears to concede that Albert does not teach this feature of claim 35 but that it would be an inherent feature of Albert's system. The Applicant agrees that the feature is not taught by Albert but respectfully disagrees with the Examiner's contention that this feature is inherent to Albert.

The system disclosed in Albert is a simple one involving one public key available to the network access device 205 and a corresponding private key held in the ISP authentication system 265. [Albert ¶ 0062] It will be shown below that neither of these keys is delivered "only if a user operating the client authenticates the user's identity with a server". The use of prior art protocols add the potential use of a symmetric key system (the RADIUS key - used between the NAS 220 and the ISP authentication system 265) and a random number (generated by the NAS 220 for use in CHAP communication) but neither of these are delivered "only if a user operating the client authenticates the user's identity with a server".

In the Basic System:

To begin with, it has been shown above that Albert does not teach the delivery of the ISP authentication system 265's public (or private) key to a client but rather simply asserts that the ISP authentication system 265's public key is known to the network access device 205. [Albert ¶ 0062] It therefore follows that, as the Examiner seems to concede, there is no discussion of a condition for delivery of the ISP authentication system 265's public (or private) key.

Using PAP/RADIUS:

The RADIUS protocol prescribes the use of symmetric encryption between the NAS 220 and the ISP authentication system 265 using the same RADIUS key at both locations. [Albert ¶ 0008, ¶ 0065] The RADIUS key is not known to the network access device 205. As mentioned above, there is no teachings in Albert regarding delivering the RADIUS key from one entity to another and it is not clear how it comes to be shared between the NAS 220 and the ISP authentication system 265. It follows that Albert does not teach delivering the RADIUS key only if a user authenticates its identity with a server.

Using CHAP/RADIUS:

The addition of the CHAP protocol dictates the use of a random number to hash the password. [Albert ¶ 0066] This random number is generated by the NAS 220 and sent to both the network access device 205 and the ISP authentication system 265. [Albert ¶ 0067] As discussed above, not only is this random number not a key, but it cannot be interpreted as a first key to which there is a second, complementary key. Furthermore, the random number is provided to the network access device 205 and to the ISP authentication system 265 without conditions and there is no authentication prior to delivery of this random number.

NPL Document:

On page 3 of the Office Action, the Examiner alleges that the above-noted feature of claim 35 is an inherent feature of Certification Authorities used in Public Key infrastructure to ensure the integrity of the network. The Applicant respectfully disagrees with the Examiner's assessment of Certification Authorities and with the implications of his assessment on claim 35.

As explained in the brief synopsis of the NPL document, above, the NPL document describes that Certificate Authorities issue digital certificates that contain the public key of a desired online resource. Once issued, a digital certificate can be held virtually anywhere accessible, without fear of tampering. [NPL document p.228, ¶ 2] Indeed digital certificates are digitally signed by the CA, using a private key known only to the CA (referred to here as the CA's private key) and nobody can alter the contents without the CA's private key (doing so will result in conspicuously incoherent data). The CA may perform its function offline and needs not be consulted when seeking a digital certificate, since digital certificates may be (and likely are) stored elsewhere than with the CA. [NPL document p.228, bullet point 1] Therefore an entity (e.g., the network access device 205), seeking to obtain the public key of an online resource (e.g. the ISP authentication system 265's public key) does not need to authenticate its identity with the CA (or anyone else) at all. Rather, it is the entity that obtains a digital certificate that does the verifying by using the CA's public key to verify the

digital signature of the digital certificate. In the example where the network access device 205 procures itself a digital certificate containing the IPS authentication system 265's public key, it is the network access device 205 itself that verifies the digital certificate's authenticity by verifying the digital signature thereof with the CA's public key.

Although not specifically disclosed in the NPL document, if an online resource such as an online banking system wants to have a digital certificate containing its own public key (the online resource's public key) emitted by a CA, it may have to verify its identity with the CA and must provide it with its own public key (the online resource's public key). However, this would be a condition for obtaining a digital certificate, not for obtaining the CA's public key. The public key of the CA is preferably known to everybody and is anyway not intended for the online resource but rather for the potential user of the online resource (the reader of digital certificates).

Furthermore, as discussed above, the NPL document deals with Certification Authorities while the Albert reference does not. Rather the Albert reference teaches a system that specifically does not require the use of CAs. Thus the Applicant respectfully submits that even if the NPL document did disclose the feature of delivering a first key to a client only if a user operating the client authenticates the user's identity with a server (which, the Applicant respectfully submits is not taught by the NPL document), it would not show that the feature is inherent in Albert. Indeed, even with the aforesaid feature present, the citation of the NPL document would remain an improper combination of prior art for a rejection under 35 USC 102(e).

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest wherein said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server.

Therefore, it is respectfully submitted that the rejection of claim 35 under 35 USC 102(e) cannot stand.

Claims 36-42 and 44 depend from independent claim 35 and as such incorporate by reference all the features contained therein. Thus, it is respectfully submitted that for the same reasons as presented above, in respect of claim 35, dependent claims 36-42 and 44 distinguish patentably over the cited prior art.

2) Claims 45-50 and 52-55

The Examiner's attention is respectfully directed towards the following features of independent claim 45:

> **Claim 45**
>
> An access controller for intermediating communications between an interface and a computer and operable to store a second key complementary to a first key; said access controller operable to communicate with a client via said interface; said client operable to store said first key and to receive instructions from a user; said access controller operable to selectively pass said instructions to said computer if a verification protocol utilizing said keys is met;
>
> wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, **a delivery of said random number and said encrypted random number from said client to said access controller**, a decryption of said encrypted random number using said second key by said access controller, **a comparison of said random number and said decrypted number**, and **a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found**.

As will be demonstrated in detail below, the Applicant respectfully submits that:

i. the cited prior art does not teach or suggest the feature of *a delivery of said random number and said encrypted random number from said client to said access controller*;

ii. the cited prior art does not teach or suggest the feature of *a comparison of said random number and said decrypted number*; and

iii. the cited prior art does not teach or suggest the features of *a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number,* and *a decision not to pass said at least a portion of said instructions if no match is found.*

I. The cited prior art does not teach or suggest the feature of a delivery of a random number and an encrypted random number from a client to an access controller

There are two possible sources of confusion regarding this feature in Albert: the random number generated under the CHAP protocol and the random point on an elliptic curve used in asymmetrical encryption.

Regarding the Random Number Used in the CHAP Protocol:
First it must be appreciated that the network access device 205 of Albert is a user end device that executes a dial-up connection (or other type of connection) application and performs no access control functions. [Albert ¶ 0059] Now as mentioned above in the synopsis of Albert, the use of the CHAP protocol prescribes the generation of a random number by the NAS 220. [Albert ¶ 0066] Here the random number is sent from the NAS 220 to the network access device 205, which uses it to hash a password. The hashed password is then sent back to the NAS 220 but without the corresponding random number. At no point does the network access device 205 send or encrypt any random number.

Furthermore, the NAS 220 itself does not send to anyone a random number and an encrypted random number. The NAS 220 sends the random number to the network access device 205 in non-encrypted form, never in encrypted form. Later, when it receives the packet containing the hashed password, the NAS 220 forwards it to the ISP authentication system 265. At this point, the NAS 220 and the ISP authentication system 265 may be communicating using the RADIUS

protocol, which, according to Albert, calls for symmetric encryption. [Albert ¶ 0008] If the packet containing the random number is encrypted, the random number portion of the packet may also be encrypted and thus the random number may be sent from the NAS 220 to the ISP authentication system 265 in encrypted form. But in such a case, there would be no sending of the random number itself, only the encrypted random number. Alternatively, the RADIUS protocol could conceivably not require encryption of the entire packet, in which case the random number may never be encrypted and only the random number itself would be sent from the NAS 220 to the ISP authentication system 265. In either case, the NAS 220 never sends a random number and an encrypted random number to any entity.

As for the ISP authentication device, it merely receives the random number and hashed password from the NAS 220 and does not send anything related to the random number externally. Internally, the network decryption server 240 sends the decrypted random number to the AAA server 235, but it does not send it an encrypted random number.

Thus, the Applicant respectfully submits that nowhere does the use of the random number required by the CHAP protocol cause the above-noted feature of claim 45 to be anticipated by Albert.

Regarding the Random Point on an Elliptic Curve Used in Elliptic Curve Cryptography:

In Albert, communication between the network access device 205 and the ISP authentication system 265 is encoded using asymmetric encryption (introduced in ¶ 0060-0061 of Albert). The specific type of asymmetric cryptography used in Albert, called elliptic curve cryptography (ECC), is illustrated in Fig. 10 and described in the text starting at paragraph 113. This algorithm begins by generating a random point on an elliptic curve. This point is named a random point, and not a random number, because it is not wholly random, being

constrained to lying on a certain elliptic curve. The point is employed to modify (encode) the password. The point itself is also encrypted and sent to a netserver (part of the ISP's systems). However, the point itself is never sent in unencrypted form. Therefore even if such a random point is interpreted as equivalent to a random number, the Albert reference fails to teach to above-noted feature of claim 45.

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest a delivery of said random number and said encrypted random number from said client to said access controller. Therefore, it is respectfully submitted that the rejection of claim 45 under 35 USC 102(e) cannot stand.

Ii. The cited prior art does not teach or suggest the feature of a comparison of the random number and the decrypted number

This particular feature requires a random number. It appears that the only possible sources of confusion in Albert are again the random number used in the CHAP protocol and the random point on an elliptic curve used in ECC.

Regarding the Random Number Used in the CHAP Protocol:
The random number is first created by the NAS 220 and sent to the network access device 205, [Albert ¶ 0066] but it is never encrypted when the RADIUS protocol is not used. In the embodiments where the RADIUS protocol is used, the NAS 220 and the ISP authentication system 265 communicate using symmetric encryption. [Albert ¶ 008, ¶ 0067] Assuming that encryption is done to all the data sent between the NAS 220 and the ISP authentication system 265, the password may be sent therebetween in encrypted form. Clearly, the NAS 220 that in such a scenario would encrypt the data is not the entity that decrypts it. Rather, the encrypted data is sent to the ISP authentication system 265 and decrypted therein by the network decryption server 240, which, as discussed above, has no

access to the original (unencrypted) random number. The network decryption server 240 therefore cannot compare the random number and the decrypted number, since it has no access to the (non-decrypted) random number. Rather, the network decryption server 240 sends the decrypted random number to the AAA server 235 [Albert ¶ 0067] (it is sent alongside the password that was hashed using the random number at the network access device 205). It is the AAA server 235 that performs the only verification regarding the random number but even there, it does not compare the decrypted number to the random number. Rather, it presumes that the decrypted number is identical to the (original) random number and uses it to hash a stored copy of the user's password. If the result matches the hashed password received from the network decryption server 240, it authorises network access for the network access device 205. [Albert ¶ 0068] At no point does the AAA server 235 or any other component of Albert compare the random number used in the CHAP protocol to a decrypted random number.

Regarding the Random Point on an Elliptic Curve Used in ECC:
As discussed above, the elliptic curve cryptography used in Albert requires the transmission of an encrypted random point on an elliptic curve, but not of the random point itself. It therefore follows that the decrypted random point, if decrypted, cannot be compared by the receiving device with the random point.

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest a comparison of said random number and said decrypted number. Therefore, it is respectfully submitted that the rejection of claim 45 under 35 USC 102(e) cannot stand.

iii. The cited prior art does not teach or suggest the features of a decision to pass at least a portion of the instructions if the comparison finds a match of the random number with the decrypted number and a decision not to pass the at least a portion of the instructions if no match is found

It has been shown that Albert fails to teach the comparison of a random number with the decrypted random number. It follows that Albert cannot teach a decision based on the comparison. Rather, in Albert, the decision of whether to grant access to the network to the network access device 205 is taken by the AAA server 235 based on the comparison of a received password with a stored password (in the Basic System and the PAP/RADIUS system) [Albert ¶ 0063, ¶ 0065] or by the comparison of a received hashed password to a hash of a stored password (in the CHAP/RADIUS system). [Albert ¶ 0068]

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number or a decision not to pass said at least a portion of said instructions if no match is found. Therefore, it is respectfully submitted that the rejection of claim 45 under 35 USC 102(e) cannot stand.

Claims 46-50 and 52-55 depend from independent claim 45 and as such incorporate by reference all the features contained therein. Thus, it is respectfully submitted that for the same reasons as presented above, in respect of claim 45, dependent claims 46-50 and 52-55 distinguish patentably over the cited prior art.

3) Claims 56-66 and 70-71

The Examiner's attention is respectfully directed towards the following feature of independent claims 56 and 70:

> **Claim 56**
> In an authentication server, a method of securing access between a client having temporary connection to a computer via an access controller, said access controller for selectively passing instructions received from said client to said

computer if a verification protocol utilizing a set of keys is met, said method comprising:

receiving a request from said access controller for an updated first key;

authenticating said request;

determining said updated first key and a second key corresponding to said updated first key; and

delivering said updated first key to said access controller.

Claim 70

An authentication server for securing access between a client having temporary connection to a computer via an access controller, said access controller for selectively passing instructions received from said client to said computer if a verification protocol utilizing a set of keys is met, said authentication server comprising:

means for receiving a request from said access controller for an updated first key;

means for authenticating said request;

means for determining said updated first key and a second key corresponding to said updated first key; and,

means for delivering said updated first key to said access controller.

As will be demonstrated in detail below, the Applicant respectfully submits that:

i. the cited prior art does not teach or suggest the feature of *receiving a request from said access controller for an updated first key*; and

ii. the Examiner has not established a basis for rejection under 35 USC 102(e) and 37 CFR 104(c)(2)

i. The cited prior art does not teach or suggest the feature of receiving a request from the access controller for an updated first key

This claim feature is absent in Albert. Instead, Albert discloses a provision for updating the ISP authentication system 265's public key stored in network access devices 205 if the corresponding ISP authentication system 265's private key is compromised. [Albert ¶ 0160] Although Albert offers no suggestion as to how it may be determined that a private key has been compromised, it puts forward a solution for replacing compromised keys involving generating a new key pair. Specifically, a new pair of ISP authentication system 265's keys (private and public) is generated and an expiry date is put on the existing compromised

keys. The expiry date is selected to be long enough to ensure that all dialers (running on the network access devices 205) [Albert ¶ 0089] log on at least one last time using the current ISP authentication system 265's current public key (which corresponds to the compromised ISP authentication system 265's private key). Once a dialer has logged on, it retrieves a new config.ini file with the new ISP authentication system 263's public key from the newly-generated key pair. [Albert ¶ 00160]

This system suffers from many drawbacks. First, it depends on the ability to set an expiry date such that all network access devices 205 will log on before the current key is removed. This, however, cannot be perfectly realised, since it is generally not possible to predict, e.g., how often people will log on to the internet using their dial-up service. Albert in particular is concerned with world-wide dial-up access, [Albert ¶ 0058, ¶ 0071] and it is possible that certain network access device 205 users may only use Albert's services when travelling, making it even harder to predict log-on intervals. However, the consequences of changing the ISP authentication system 265's key pair before all users have had a chance to update their copy of the ISP authentication system 265's public key are relatively serious: those users that did not log-on before the expiry of the old key, will find themselves unable to log on since their copy of the ISP authentication system 265's public key will no longer encrypt their password in a way the ISP can understand. Also, in the interval between the time the ISP authentication system 265's private key has been found to be compromised and the expiry of the current ISP authentication system 265's key pair, any potential intruder (it is presumed there are intruders, since the key is compromised) has free reign in the system.

Advantageously, the present invention involves "receiving a request from said access controller for an updated first key". Thus the access controller can request, whenever appropriate, an updated first key, which key is determined

(along with a second key) and delivered. This feature is completely absent from Albert.

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest receiving a request from the access controller for an updated first key. Therefore, it is respectfully submitted that the rejection of claims 56 and 70 under 35 USC 102(e) cannot stand.

ii. The Examiner has not established a basis for rejection under 35 USC 102(e) and 37 CFR 104(c)(2)

On page 5 of the Office Action mailed January 10, 2008, the Examiner rejected claims 45-82 under 35 USC 102(e) but gave no basis for the rejection. Instead the Examiner merely stated "claims 45-82 do not teach or define any new limitations beyond the claims above [claims 35-42 and 44], therefore, they are rejected for similar reasons." Respectfully, the Applicant submits that this statement is erroneous. In his rejection the Examiner assumes that all the features of claims 56 and 70 are recited in claims 35-42 and 44, however the Applicant respectfully submits that this is not the case. Specifically, the above-emphasized feature of claims 56 and 70 is absent from claims 35-42 and 44. There is therefore at least one feature of rejected claims 56 and 70 that is not recited in the claims referred to by the Examiner. Accordingly, the Applicant respectfully submits that there were no grounds for the Examiner's rejection of claims 56 and 70 in the Office Action mailed January 10, 2008.

The absence of grounds for the rejection of claims 56 and 70 was pointed out in the Applicant's letter of March 7, 2008. In response, the Examiner has referred, in the Advisory Action of March 28, 2008, to a statement in the Office Action encouraging the Applicant to consider the reference in its entirety. He also added an allegation that "Albert does in fact teach key updating, and dealing with expiry

of a verification protocol as claimed (refer to paragraph 0060-0061 and 0161) and therefore meet the scope of the claimed limitation."

Firstly, it is respectfully submitted that the Applicant did consider the reference in its entirely and, as discussed above, it was found not to be anticipating claims 56-66 and 70-71. Secondly, the Applicant respectfully submits that the Examiner has not met the requirements of 37 CFR 104(c)(2) which states:

> *In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified.*

In particular, the Examiner has not properly designated the part of Albert that the rejection relies on nor provided indication as to how Albert, which pertains to a system for an Internet Service Provider to verify the identity of dial-up internet customers prior to providing them access to the internet with the ISP's equipment, may be pertinent to claims 56 and 70. His above-quoted statement in the Advisory Action of March 7, 2008, merely contained and allegation that the claim is anticipated and a reference to apparently irrelevant sections of Albert.

A mere statement alleging that the claim is anticipated does not satisfy the requirements of 37 CFR 104(c)(2) and 35 USC 102(e). Furthermore, the sections of Albert pointed out by the Examiner do not appear relevant to claims 56 and 70 and neither support a rejection under 35 USC 102(e) nor provide for the requirements of 37 CFR 104(c)(2). Indeed, paragraphs 0060-0061 merely explain that a user password in Albert is encrypted using prior art asymmetric key cryptography and describe briefly how such cryptography works. Paragraph 0161 regards changing a public key in a dialer when the corresponding private key has been compromised and has nothing to do with updating a public key upon any

request. Therefore the cited passages do not contribute to show how the prior art anticipates claims 56 and 70.

In light of the absence of explanation as to how claims 56 and 70 are anticipated, the Applicant respectfully submits that the Examiner has not met his burden under 37 CFR 104(c)(2) and that the rejection under 35 USC 102(e) is improper. Withdrawal of the rejection and allowance of claims 56 and 70 is respectfully solicited.

Claims 57-66 and 71 depend from independent claims 56 and 70 respectively and as such incorporate by reference all the features contained therein. Thus, it is respectfully submitted that for the same reasons as presented above, in respect of claims 56 and 71, dependent claims 57-66 and 71 distinguish patentably over the cited prior art.

4) Claim 67

The Examiner's attention is respectfully directed towards the following features of independent claim 67:

Claim 67

A method of securing access between a client and a computer having an access controller intermediate said client and said computer, said method comprising:

receiving an instruction at said client destined for said computer;

generating a random number by said client;

encrypting said random number by said client using a first key;

delivering said random number, said encrypted random number and said instruction to said access controller;

decrypting said encrypted random number using a second key by said access controller, said second key complementary to said first key;

comparing said random number and said decrypted number;

passing at least a portion of said instruction to said computer if said comparison finds a match of said random number with said decrypted number; and,

discarding said at least a portion if no match is found.

As will be demonstrated in detail below, the Applicant respectfully submits that:

i. the cited prior art does not teach or suggest the feature of *delivering said random number, said encrypted random number and said instruction to said access controller*;

ii. the cited prior art does not teach or suggest the feature *of comparing said random number and said decrypted number*; and

iii. the cited prior art does not teach or suggest the features of *passing at least a portion of said instruction to said computer if said comparison finds a match of said random number with said decrypted number;* and, *discarding said at least a portion if no match is found.*

i. The cited prior art does not teach or suggest the feature of delivering a random number, an encrypted random number and an instruction to an access controller

It has been shown above, under subheading (i) of the discussion pertaining to claim 45, that Albert does not disclose a delivery of a random number and an encrypted random number to an access controller. It therefore follows that neither reference teaches delivering a random number, an encrypted random number and an instruction to an access controller. Therefore, for the same reasons as presented above in the discussion pertaining to claim 45, and applying the same arguments as presented there, the Applicant respectfully submits that the above-underlined feature of claim 67 is completely absent from the cited prior art.

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest delivering a random number, an encrypted random number and an instruction to an access controller. Therefore, it is respectfully submitted that the rejection of claim 67 under 35 USC 102(e) cannot stand.

ii. The cited prior art does not teach or suggest the feature of comparing said random number and said decrypted number

It has been shown above, under subheading (ii) of the discussion pertaining to claim 45, that Albert does not disclose a comparison of a random number and a decrypted number. The arguments presented there equally show that Albert does not disclose comparing said random number and said decrypted number. Therefore, for the same reasons as presented above in the discussion pertaining to claim 45, and applying the same arguments as presented there, the Applicant respectfully submits that Albert does not teach or suggest comparing the above-underlined feature of claim 67.

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest comparing said random number and said decrypted number. Therefore, it is respectfully submitted that the rejection of claim 67 under 35 USC 102(e) cannot stand.

iii. The cited prior art does not teach or suggest the features of passing at least a portion of said instruction to said computer if said comparison finds a match of said random number with said decrypted number and discarding said at least a portion if no match is found

It has been shown above, under subheading (iii) of the discussion pertaining to claim 45, that Albert does not disclose a decision to pass at least a portion of instructions if a comparison finds a match of a random number with a decrypted random number or a decision not to pass the at least a portion of the instructions if no match is found. The arguments presented there equally show that Albert does not disclose passing at least a portion of said instructions to said computer if said comparison finds a match of said random number with said decrypted number or discarding said at least a portion if no match is found. Therefore, for the same reasons as presented above in the discussion pertaining to claim 45,

and applying the same arguments as presented there, the Applicant respectfully submits that Albert does not teach or suggest the above-underlined feature of claim 67.

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest either the feature of passing at least a portion of said instruction to said computer if said comparison finds a match of said random number with said decrypted number or the feature of discarding said at least a portion if no match is found. Therefore, it is respectfully submitted that the rejection of claim 67 under 35 USC 102(e) cannot stand.

5) Claims 68-69

The Examiner's attention is respectfully directed towards the following feature of independent claim 68:

> **Claim 68**
> An authentication server, comprising:
> an interface for communicating with a client and an access controller via a communication medium; and
> a processing unit operable to determine a first key for delivery to said client and a second key for delivery to said access controller, **said first key being delivered to said client only if a user operating said client authenticates said user's identity with said server**; such that when said access controller and said client are connected, said access controller selectively passes instructions from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met.

As will be demonstrated in detail below, the Applicant respectfully submits that:

i. the combination of Albert and the NPL document in a rejection under 35 USC 102(e) is improper; and

ii. the cited prior art does not teach or suggest the feature *of said first key being delivered to said client only if a user operating said client authenticates said user's identity with said server.*

I. The combination of Albert and the NPL document in a rejection under 35 USC 102(e) is improper

In his rejection of claim 35 under 35 USC 102(e), the Examiner has combined Albert with the NPL document, alleging that the NPL document shows that the feature of "wherein said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server" is actually inherent in Albert though not expressly disclosed. On page 5 of the Office Action mailed January 10, 2008, the Examiner alleges that claims 45-82 "do not teach or define any new limitations beyond [claims 35-42 and 44], therefore, they are rejected for similar reasons." Furthermore, in the Advisory Action mailed March 28, 2008, the Examiner did not present any additional arguments supporting his rejection of claims 68-69. Since the Examiner relied on the NPL document to contend that a feature of claim 35 is inherent in Albert, since this feature is equally present in claim 68 and since the Examiner applies the same reasoning in his rejection of claim 68 (and dependent claim 69) as applied to the rejection of claims 35-42 and 44, it follows that the Examiner relies equally on the NPL document in his rejection of claims 68-69.

As discussed above, under subheading (i) of the discussion pertaining to claim 35, the Applicant respectfully disagrees with the Examiner's interpretation of the prior art and submits that the NPL document is concerned with different technology than Albert and thus cannot be used to show that a feature is inherent in Albert.

As mentioned above, the NPL document provides a basic introduction to Certification Authorities, which are third party systems used to counter the emission of fake public keys online. [NPL document, p.228, ¶ 2]. Albert, on the other hand, relates to a self-contained system for authorising access to an online resource. In particular, Albert provides a system for verifying the identity of users

of dial-up internet service when they log on to the internet. Advantageously, the verification method provided can be used by the ISP without substantial recourse to external services, even when the user is logging into a foreign network. [Albert ¶ 0058, ¶ 0071] One of the objectives of Albert is to provide a system that does not require the use of external services such as Certification Authorities, the need of which is specifically pointed out as a disadvantage of the art prior to Albert (see paragraph 0014).

Besides specifically teaching away from employing Certification Authorities, the Albert reference does not teach anything that resembles a CA. To begin with, Albert does not aim to protect a public key at all but rather to protect, by encryption, the password of a user logging on. [Albert ¶ 0056] Whereas CAs protect users from supposititious online resources, Albert aims to protect an online resource from unauthorized users.

Albert achieves his goal by having the password encrypted at the user end (network access device 205) before sending it to an ISP authentication system 265 that decrypts it and decides whether or not to allow access to a resource (the internet). [Albert ¶ 0055] In contrast, a Certification Authority merely generates digital certificates comprising a public key for an online resource. The digital certificate is not used by the online resource provider to determine if a user is entitled to access the online resource, rather it is used by a user to find out the online resource's public key. [NPL document, p.228, ¶ 2] The key allows the user to communicate safely with the online resource but is generally available to everyone (who has the CA's public key). However, having the online resource's public key does not mean that the user will be allowed access to the corresponding online resource.

The NPL document also describes, on page 227, Key Distribution Centers (KDCs), which are more primitive alternatives to CAs. But the section on KDCs is not relied upon by the Examiner and is only used within the NPL document to

provide context for the discussion on CAs. Furthermore, KDCs are even more conceptually distant from the Albert system than CAs and thus there is no need to discuss KDCs in further detail here.

In the Advisory Action mailed March 28, 2008, the Examiner states that he employs the NPL reference in accordance with MPEP 2131.01 in order to show that a characteristic not disclosed in Albert is actually inherent in the Albert system. Yet Albert discloses a system that is significantly different than a CA and that does not use CAs. The Applicant respectfully submits that since Albert does not teach or employ Certification Authorities or like structures (or KDCs), a document describing only such Certification Authorities (and KDCs) cannot possibly show that any particular feature is inherent in the Albert system.

In light of the foregoing, the Applicant respectfully submits that the Examiner improperly combined documents for his rejection under 35 USC 102(e) and that accordingly, the rejection of claim 68 cannot stand.

ii. The cited prior art does not teach or suggest the feature of said first key being delivered to said client only if a user operating said client authenticates said user's identity with said server

It has been shown above, under subheading (iv) of the discussion pertaining to claim 35 that Albert does not disclose *said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server.* The arguments presented there equally show that Albert does not disclose *a first key being delivered to a client only if a user operating the client authenticates the user's identity with the server.* Therefore, for the same reasons as presented above in the discussion pertaining to claim 35, and applying the same arguments as presented there, the Applicant respectfully submits that Albert does not teach or suggest comparing the above-underlined feature of claim 68.

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest said first key being delivered to said client only if a user operating said client authenticates said user's identity with said server. Therefore, it is submitted that the rejection of claim 68 under 35 USC 102(e) cannot stand.

Claim 69 depends from independent claim 68 and as such incorporates by reference all the features contained therein. Thus, it is respectfully submitted that for the same reasons as presented above, in respect of claim 68, dependent claim 69 distinguishes patentably over the cited prior art.

6) Claims 72-73

The Examiner's attention is respectfully directed towards the following features of independent claim 72:

> **Claim 72**
> In an access controller for selectively passing instructions between a client and a computer if a verification protocol is met, a method of expiring said verification protocol, comprising:
> **determining if a first preset period of time since said client disconnected from said access controller has elapsed;**
> **determining if a second preset period of time since said verification protocol was updated has elapsed; and,**
> **expiring said verification protocol by refusing to pass said instructions if either of said preset periods of time have elapsed.**

As will be demonstrated in detail below, the Applicant respectfully submits that:

i. the cited prior art does not teach or suggest the feature of *determining if a first preset period of time since said client disconnected from said access controller has elapsed*;

ii. the cited prior art does not teach or suggest the feature of *determining if a second preset period of time since said verification protocol was updated has elapsed*;

iii. the cited prior art does not teach or suggest the feature of *expiring said verification protocol by refusing to pass said instructions if either of said preset periods of time have elapsed*; and

iv. the Examiner has failed to establish anticipation by the prior art.

i. The cited prior art does not teach or suggest the feature of determining if a first preset period of time since a client disconnected from an access controller has elapsed

This feature of claim 72 is absent in Albert. As mentioned above in the discussion pertaining to claims 56-66 and 70-71, the Albert system includes a provision for updating the copy of the ISP authentication system 265's public keys held by network access devices 205 if the corresponding ISP authentication system 265's private key is compromised. [Albert ¶ 0160] Albert, however, offers no suggestion at all as to how it may be determined that the ISP authentication system 265's private key has been compromised and does not provide a way of deciding when to update keys or any other aspect of a security mechanism. Rather, Albert focuses only on how to update ISP authentication system 265's keys and doesn't teach when to do so.

Specifically, Albert teaches generating a new pair of ISP authentication system 265's keys (public and private) when the current pair is compromised (the pair is said to be compromised when the private key, which must remain secret, is compromised). The system then sets an expiry date for the current (compromised) pair of ISP authentication system 265's keys. [Albert ¶ 0161] Once the expiry date is reached, the compromised ISP authentication system 265's key pair is replaced with the newly generated key pair. Meanwhile, in the time between the generation of the new ISP authenticaiton system 265's key pair and the expiry date, the copy of the ISP authentication system 265's public key held on all dialers (which are running on the network access devices 205 [Albert ¶ 0089]) is updated upon log-on. Once a dialer has logged on, it retrieves a new

config.ini file with a copy of the new ISP authentication system 265's public key. [Albert ¶ 0160] The expiry date is selected to be long enough to ensure that all dialers log on one last time using the current (compromised) key so that all get a chance to receive a copy of the new ISP authentication system 265's public key before the current one expires. [Albert ¶ 0161]

This updating is done, however, only upon discovery that a private key has been compromised [Albert ¶ 0160] and not upon any other event nor on any regular basis. It will be appreciated that the expiry date in Albert is an arbitrarily-set time representing a delay between the time the ISP authentication system 265's private key is found to be compromised and the time the system switches to a new non-compromised pair of ISP authentication system 265's keys. [Albert ¶ 0161] This delay is created to give a chance to all the dialers (running on network access devices 205 [Albert ¶ 0089]) to update their copy of the ISP authentication system 265's public key before it becomes obsolete. In other words, the delay created by the expiry date in Albert is essentially a time frame in which it is expected everyone will connect at least once –this time frame may be very large. This time frame, however, is not related to the time since an entity (client or otherwise) has disconnected from an other entity (access controller or otherwise). Nor is this delay used for any preventative measure (such as to ensure that a once-used key is not re-used by an intruder) at all.

As mentioned above, in the discussion pertaining to claims 56 and 70, the Albert system suffers many drawbacks. Another drawback is that it takes a reactive approach to security, expiring keys only after they have been found to be compromised. During the time delay between the discovery that the ISP authentication system 265's private key has been compromised and the expiry of the ISP authentication system 265's pair of keys, any potential intruder (it is presumed that there are intruders, since the key is compromised) has free reign in the system.

By failing to take into account network activity (e.g. client connection/disconnection) and security activity (e.g. last update) in deciding whether to update the ISP authentication system 265's public/private key pair, Albert causes major security deficiencies.

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest determining if a first preset period of time since said client disconnected from said access controller has elapsed. Thus, it is respectfully submitted that the rejection of claim 72 under 35 USC 102(e) cannot stand.

ii. The cited prior art does not teach or suggest the feature of determining if a second preset period of time since a verification protocol was updated has elapsed

As mentioned under subheading (i) above, expiry of a key in Albert is done only upon discovery that a private key has been compromised. [Albert ¶ 0160] The only time constraint related to expiry of a compromised key disclosed in Albert is a delay between the time the ISP authentication system 265's private key is found to be compromised and the time the key (and corresponding public key) is expired. [Albert ¶ 0161] Thus Albert is completely silent on any second preset period of time.

Furthermore, it will be appreciated that the expiry date in Albert has nothing to do with the time since a verification protocol was updated. Rather, the delay preceding the expiry serves to allow the different users of the system to log on using the soon-to-be-expired ISP authentication system 265's public key at least one last time and to obtain the new ISP authentication system 265's public key to be used after the expiry. [Albert ¶ 0161] Thus, this delay relates to an expected time period during which all users will connect at least once, not to previous key expiry or protocol updates.

It will also be appreciated that the delay resulting from the expiry date is not used to decide to expire a verification protocol. Rather, once the decision is already made to expire a pair of encryption keys, the expiry date in Albert determines when in the future this expiry will take place. [Albert ¶ 0160]

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest determining if a second preset period of time since said verification protocol was updated has elapsed. Thus, it is respectfully submitted that the rejection of claim 72 under 35 USC 102(e) cannot stand.

iii. The cited prior art does not teach or suggest the feature of expiring said verification protocol by refusing to pass said instructions if either of said preset periods of time have elapsed

First, it has been shown under subheadings (i) and (ii) above that Albert does not teach the claimed preset periods of time. It follows from that alone that Albert cannot teach expiring a verification protocol (by any means) if either of the preset periods of time have elapsed.

Furthermore, in Albert, the only expiry that takes place is expiry of the ISP authentication system 265's public/private key pair. [Albert ¶ 0160] The process of expiring the key pair involves creating a time window (the delay caused by the expiry date) during which all dialers (running on network access devices 205 [Albert ¶ 0089]) receive a new ISP authentication system 265's public key, and replacing the ISP authentication system 265's private key with a new one at the end of the time window. [Albert ¶ 0161] Once this done, all network access devices 205 should be communicating with the ISP authentication system 265 using the ISP authentication system 265's new public key and anybody using the old key should be unable to communicate with the ISP authentication system 265. It will be appreciated that this method for expiring a public/private key pair

taught by Albert is not equivalent to expiring a verification protocol by refusing to pass instructions.

In light of the foregoing, the Applicant respectfully submits that the cited prior art does not teach or suggest expiring said verification protocol by refusing to pass said instructions if either of said preset periods of time have elapsed. Thus, it is respectfully submitted that the rejection of claim 72 under 35 USC 102(e) cannot stand.

iv. The Examiner has not established a basis for rejection under 35 USC 102(e) and 37 CFR 104(c)(2)

On page 5 of the Office Action mailed January 10, 2008, the Examiner rejected claims 45-82 under 35 USC 102(e) but gave no basis for the rejection. Instead the Examiner merely stated "claims 45-82 do not teach or define any new limitations beyond the claims above [claims 35-42 and 44], therefore, they are rejected for similar reasons." Respectfully, the Applicant submits that this statement is erroneous. In his rejection the Examiner assumes that all the features of claim 72 are recited in claims 35-42 and 44, however the Applicant respectfully submits that this is not the case. Specifically, the above-emphasized features of claim 72 are absent from claims 35-42 and 44. There is therefore at least one feature of rejected claim 72 that is not recited in the claims referred to by the Examiner. Accordingly, the Applicant respectfully submits that there were no grounds for the Examiner's rejection of claim 72 in the Office action mailed January 10, 2008.

The absence of grounds for the rejection of claims 72 was pointed out in the Applicant's letter of March 7, 2008. In response, the Examiner has referred, in the Advisory Action of March 28, 2008, to a statement in the Office Action encouraging the Applicant to consider the reference in its entirety. He also added an allegation that "Albert does in fact teach key updating, and dealing with expiry

of a verification protocol as claimed (refer to paragraph 0060-0061 and 0161) and therefore meet the scope of the claimed limitation."

Firstly, it is respectfully submitted that the Applicant did consider the reference in its entirety and, as discussed above, it was found not to be anticipating claims 72-73. Secondly, the Applicant respectfully submits that the Examiner has not met the requirements of 37 CFR 104(c)(2) which states:

> *In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified.*

In particular, the Examiner has not properly designated the part of Albert that the rejection relies on nor provided indication as to how Albert, which pertains to a system for an Internet Service Provider to verify the identity of dial-up internet customers prior to providing them access to the internet with the ISP's equipment, may be pertinent to claim 72. His above-quoted statement in the Advisory Action of March 7, 2008, merely contained an allegation that the claim is anticipated and a reference to apparently irrelevant sections of Albert.

A mere statement alleging that the claim is anticipated does not satisfy the requirements of 37 CFR 104(c)(2) and 35 USC 102(e). Furthermore, the sections of Albert pointed out by the Examiner do not appear relevant to claim 72 and neither support a rejection under 35 USC 102(e) nor provide for the requirements of 37 CFR 104(c)(2). Indeed, paragraphs 0060-0061 merely explain that a user password in Albert is encrypted using prior art asymmetric key cryptography and describe briefly how such cryptography works. Paragraph 0161 regards a method of changing a public key in a dialer when the corresponding private key has been compromised and has nothing to do with determination of whether to expire a verification protocol or with either of the time periods defined in claim 72.

Therefore the cited passages do not contribute to show how the prior art anticipates claim 72.

In light of the absence of explanation as to how claim 72 is anticipated, the Applicant respectfully submits that the Examiner has not met his burden under 37 CFR 104(c)(2) and that the rejection under 35 USC 102(e) is improper. Withdrawal of the rejection and allowance of claim 72 is respectfully solicited.

Claim 73 depends from independent claim 72 and as such incorporates by reference all the features contained therein. Thus, it is respectfully submitted that for the same reasons as presented above, in respect of claim 72, dependent claim 73 distinguishes patentably over the cited prior art.

7) Claims 74-82

The Examiner's attention is respectfully directed towards the following features of independent claim 74:

> **Claim 74**
> An authentication system, comprising:
> an access controller operable to communicate with a client via a first communication medium;
> an authentication server operable to communicate with said client and said access controller via a second communication medium and further **operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key** such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys; and wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met;
> wherein said access controller contains a preset second key and said authentication server maintains a record of said preset second key; **said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof.**

As will be demonstrated in detail below, the Applicant respectfully submits that:

i. the cited prior art does not teach or suggest the feature of *an authentication server operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key*; and

ii. the cited prior art does not teach or suggest the feature of *said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof.*

i. The cited prior art does not teach or suggest the feature of an authentication server operable to deliver a first key to a client and a second key to an access controller, said second key being complementary to said first key

This has been shown above, under subheading (ii) of the discussion pertaining to claim 35. Thus, for the same reasons as those presented above in section 1), it is respectfully submitted that the rejection of claim 74 under 35 US 102(e) cannot stand.

ii. The cited prior art does not teach or suggest the feature of an access controller that contains a preset second key and an authentication server that maintains a record of said preset second key, the authentication server being operable to deliver the first key and the second key only if the access controller successfully transmits the preset second key to the authentication server and the transmitted preset second key matches the authentication server's record thereof

In the Basic System:

Albert contemplates a public key (held at the network access device 205) and a private key (held at the decryption server in the ISP authentication system 265).

To begin with, it is submitted that a person of ordinary skill in the art would not consider the user or the network access device 205 in this scenario to be an access controller. Nevertheless, even if the user or the network access device 205 in this scenario were interpreted as an "access controller", neither entity is required to transmit a key (preset or otherwise). Rather, the user's encrypted password is transmitted and it is this password that is eventually decrypted and matched to a record held at the ISP authentication system 265. Nowhere is there any suggestion of storing a record of a key and matching a transmitted key with a record thereof.

Furthermore, for the aforesaid feature to be present in Albert, the ISP authentication system 265, a component thereof, or another element would need to "be operable to deliver [a] first key and [a] second key." Yet in the basic system, Albert does not suggest that the ISP authentication system 265 (or any other element) deliver any encryption key to any recipient. Rather, Albert merely discloses that the network access device 205 knows the ISP authentication system 265's public key (see the first three lines of ¶ 0062 in Albert). There is no indication, however of where the private/public keys are generated and there is no indication that a key is sent to the network access device 205 from the ISP authentication system 265 (or vice versa). Yet even if Albert did teach the ISP authentication system 265 sending the public key to the network access device 205, a skilled reader would still not be brought closer to the claimed invention since neither ISP authentication system 265 nor any constituent part thereof delivers a second key to any recipient whatsoever. There is therefore no delivery of a second key.

As shown below, combining the Albert system with the prior art PAP/RADIUS and CHAP/RADIUS protocols still does not yield the above-underlined feature of claim 74.

Using PAP/RADIUS:

If the PAP and RADIUS protocols are used with the Albert system, communications between the ISP authentication system 265 and the NAS 220 are done using the RADIUS protocol which, according to Albert, calls for symmetric encryption. Thus where Albert describes using the RADIUS protocol, it does not provide any teachings that would bring a skilled reader closer to the claimed invention.

The use of PAP/RADIUS adds the element of symmetric encryption between the NAS 220 and the ISP authentication system 265, but this does result in Albert having the above-noted feature of claim 74. Albert explains that here, encryption/decryption is done at both ends using the same key; which shall be referred to herein as the RADIUS key. [Albert ¶ 008, ¶ 0065] Albert does not provide any indication as to how the NAS 220 and the ISP authentication system 265 come to agree on the common RADIUS key to be used and Albert does not suggest that the ISP authentication system 265, or any constituent thereof, delivers the RADIUS key to the NAS 220 (or vice versa). (see ¶ 0065, where the use of RADIUS is explained). Thus no part of the RADIUS protocol implies the delivery of a first key and a second key only upon transmission of another key (preset or otherwise). Furthermore, nowhere is there any suggestion of storing a record of a RADIUS key and matching a transmitted RADIUS key with a record thereof.

Using CHAP/RADIUS:

Using CHAP calls for the generation of a random number, presumably at every attempt by a user to log on. This random number is generated and delivered at each log-on and, being random, it has no relation to any previous random number or to any other preset key. [Albert ¶ 0066] Furthermore, none of the entities that receive the random number (including the network access device 205, the ISP authentication system 265, the network decryption server 240 and the AAA server 235) have any record of the random number prior to receiving it. The NAS 220 that generates and sends the random number never receives it or

a copy of it from any other entity. Thus, even if the CHAP random number is perceived as a key, the use of the CHAP cannot imply the matching of a transmitted key with a record thereof since no entity in Albert is ever in possession of both a transmitted random number and a received record thereof.

In light of the foregoing, the Applicant respectfully submits that the cited prior Art does not teach or suggest said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof. Therefore, it is respectfully submitted that the rejection of claim 74 under 35 USC 102(e) cannot stand.

Claims 75-82 depend from independent claim 74 and as such incorporate by reference all the features contained therein. Thus, it is respectfully submitted that for the same reasons as presented above, in respect of claim 74, dependent claims 75-82 distinguish patentably over the cited prior art.

VIII. 37 CFR §41.37 (c)(1)(viii) - Claim Appendix

The following is a listing of the claims involved in the present appeal.

1. – 34. (*cancelled*)

35. An authentication system, comprising:

an access controller operable to communicate with a client via a first communication medium; and

an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys; and wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met;

wherein said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server.

36. The authentication system according to claim 35, wherein said authentication server is operable to generate said first key and said second key.

37. The authentication system according to claim 35, wherein said first key is a public encryption key and said second key is a private encryption key complementary to said public encryption key.

38. The authentication system according to claim 35, wherein each of said first communication medium and said second communication medium is selected from the group of networks consisting of the Internet, the PSTN, a local area network, and a wireless network.

39. The authentication system according to claim 35, wherein said computer is a telecommunications switch.

40. The authentication system according to claim 35, wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found.

41. The authentication system according to claim 35, wherein said instructions are encrypted by said client using said first key and said verification protocol is based on a successful decryption of said instructions by said access controller using said second key.

42. The authentication system according to claim 35, wherein said first key is delivered to said client only after said second key has been successfully delivered to said access controller.

43. (*cancelled*)

44. The authentication system according to claim 35, wherein said access controller contains a preset second key and said authentication server maintains a record of said preset second key; said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof.

45. An access controller for intermediating communications between an interface and a computer and operable to store a second key complementary to a first key; said access controller operable to communicate with a client via said interface; said client operable to store said first key and to receive instructions from a user; said access controller operable to selectively pass said instructions to said computer if a verification protocol utilizing said keys is met;

wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted

number, and a decision not to pass said at least a portion of said instructions if no match is found.

46. The access controller of claim 45, wherein said access controller is operable to obtain said second key from an authentication server and said client is operable to obtain said first key from said authentication server.

47. The access controller of claim 46, wherein said authentication server is operable to generate said first key and said second key.

48. The access controller of claim 45, wherein said first key is a public encryption key and said second key is a private encryption key complementary to said public encryption key.

49. The access controller of claim 45, wherein a medium for connecting said interface and said client is selected from the group consisting of an RS-232 cable, a USB cable, the Internet, the PSTN, a local area network, and a wireless network.

50. The access controller of claim 45, wherein said computer is a telecommunications switch.

51. (*cancelled*)

52. The access controller of claim 45, wherein said instructions are encrypted by said client using said first key and said verification protocol is based on

a successful decryption of said instructions by said access controller using said second key.

53. The access controller of claim 46, wherein said first key is obtained by said client only after said second key has been successfully obtained by said access controller.

54. The access controller of claim 46, wherein said first key is obtained by said client only if a user operating said client authenticates said user's identity with said authentication server.

55. The access controller of claim 46, wherein said access controller contains a preset second key and said authentication server maintains a record of said preset second key; said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof.

56. In an authentication server, a method of securing access between a client having temporary connection to a computer via an access controller, said access controller for selectively passing instructions received from said client to said computer if a verification protocol utilizing a set of keys is met, said method comprising:

receiving a request from said access controller for an updated first key;

authenticating said request;

determining said updated first key and a second key corresponding to said updated first key; and

delivering said updated first key to said access controller.

57. The method of claim 56, further comprising:

receiving a second request from said client for said second key;

authenticating said second request;

delivering said second key to said client.

58. The method according to claim 56, wherein determining said updated first key and said second key includes generating said updated first key and said second key.

59. The method according to claim 56, wherein said updated first key is a private encryption key and said second key is a public encryption key complementary to said private encryption key.

60. The method according to claim 56, wherein a communication medium between at least one of said authentication server, said access controller and said client is selected from the group of networks consisting of the Internet, the PSTN, a local area network, and a wireless network.

61. The method according to claim 56, wherein said computer is a telecommunications switch.

62. The method according to claim 56, wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said second key, a delivery of

said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted number using said updated first key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found.

63. The method according to claim 56, wherein said instructions are encrypted by said client using said second key and said verification protocol is based on a successful decryption of said instructions by said access controller using said updated first key.

64. The method according to claim 57, wherein said second key is delivered to said client only after said updated first key has been verified as having been successfully delivered to said access controller.

65. The method according to claim 57, wherein said second key is delivered to said client only if a user operating said client authenticates said user's identity with said authentication server.

66. The method according to claim 57, wherein said access controller contains a preset first key and said authentication server maintains a record of said preset first key; said authentication server operable to deliver said updated first key and said second key only if said access controller successfully transmits said preset first key to said authentication server and said transmitted preset first key matches said authentication server's record thereof.

67. A method of securing access between a client and a computer having an access controller intermediate said client and said computer, said method comprising:

receiving an instruction at said client destined for said computer;

generating a random number by said client;

encrypting said random number by said client using a first key;

delivering said random number, said encrypted random number and said instruction to said access controller;

decrypting said encrypted random number using a second key by said access controller, said second key complementary to said first key;

comparing said random number and said decrypted number;

passing at least a portion of said instruction to said computer if said comparison finds a match of said random number with said decrypted number; and,

discarding said at least a portion if no match is found.

68. An authentication server, comprising:

an interface for communicating with a client and an access controller via a communication medium; and

a processing unit operable to determine a first key for delivery to said client and a second key for delivery to said access controller, said first key being delivered to said client only if a user operating said client authenticates said user's identity with said server; such that when said access controller and said client are connected, said access controller selectively passes instructions from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met.

69. The authentication server of claim 68, wherein said processing unit is operable to generate said first key and said second key.

70. An authentication server for securing access between a client having temporary connection to a computer via an access controller, said access controller for selectively passing instructions received from said client to said computer if a verification protocol utilizing a set of keys is met, said authentication server comprising:

means for receiving a request from said access controller for an updated first key;

means for authenticating said request;

means for determining said updated first key and a second key corresponding to said updated first key; and,

means for delivering said updated first key to said access controller.

71. The authentication server of claim 70, wherein said means for determining said updated first key and said second key is operable to generate said updated first key and said second key.

72. In an access controller for selectively passing instructions between a client and a computer if a verification protocol is met, a method of expiring said verification protocol, comprising:

determining if a first preset period of time since said client disconnected from said access controller has elapsed;

determining if a second preset period of time since said verification protocol was updated has elapsed; and,

expiring said verification protocol by refusing to pass said instructions if either of said preset periods of time have elapsed.

73. The method according to claim 72, wherein said verification protocol utilizes a first encryption key respective to said client and a second encryption key respective to said access controller and said expiring step includes an instruction to said access controller to refuse to accept communications from said client that utilize said first encryption key.

74. An authentication system, comprising:

an access controller operable to communicate with a client via a first communication medium; and

an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys; and wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met;

wherein said access controller contains a preset second key and said authentication server maintains a record of said preset second key; said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof.

75. The authentication system according to claim 74, wherein said authentication server is operable to generate said first key and said second key.

76. The authentication system according to claim 74, wherein said first key is a public encryption key and said second key is a private encryption key complementary to said public encryption key.

77. The authentication system according to claim 74, wherein each of said first communication medium and said second communication medium is selected from the group of networks consisting of the Internet, the PSTN, a local area network, and a wireless network.

78. The authentication system according to claim 74, wherein said computer is a telecommunications switch.

79. The authentication system according to claim 74, wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found.

80. The authentication system according to claim 74, wherein said instructions are encrypted by said client using said first key and said verification protocol is based on a successful decryption of said instructions by said access controller using said second key.

81. The authentication system according to claim 74, wherein said first key is delivered to said client only after said second key has been successfully delivered to said access controller.

82. The authentication system according to claim 74, wherein said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server.

IX. 37 CFR §41.37 (c)(1)(ix) - Evidence Appendix

There is no evidence submitted herewith.

X. 37 CFR §41.37 (c)(1)(x) - Related Proceedings Appendix

There are no related proceedings at per paragraph c(1)(ii) indicated above.

CONCLUSION

It is respectfully submitted that all of claims 35-42, 44-50 and 52-82 are in condition for allowance as they currently stand. Reconsideration of the rejections and objections is requested. Allowance of claims 35-42, 44-50 and 52-82 at an early date is solicited.

Respectfully submitted,

Dated: July 10, 2008

Sanro Zlobec
Reg. No. 52,535
Agent for the Applicant

SMART & BIGGAR
1000 De La Gauchetière Street West
Suite 3300
Montreal, Quebec H3B 4W5
CANADA

Customer Number: 28291

Telephone: (514) 954-1500
Facsimile: (514) 954-1396